AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims, in which claims 1, 10, 19 and 28 are currently amended.

1. (Currently Amended) A network apparatus for performing functions to enhance performance of a communication network, comprising:

a spoofing module configured to selectively spoof a plurality of connections associated with a plurality of hosts based upon corresponding spoofing criteria and to provide local acknowledgement of received messages over the connections;

a connection module configured to multiplex the plurality of connections over a common backbone connection;

a prioritization module configured to prioritize access to the backbone connection based upon prioritization criteria;

a path selection module configured to determine a path among a plurality of paths to transmit the received messages based upon path selection criteria and

a data compression module configured to apply compression on individual ones of the connections or the backbone connection, wherein the data compression module concurrently applies different types of compression on the individual connections.

2. (Previously Presented) The network apparatus according to claim 4, further comprising:

a mapping table to store connection control block allocation information.

3. (Previously Presented) The network apparatus according to claim 4, further comprising:

a hash function logic configured to output pointers corresponding to the plurality of connection control blocks.

4. (Previously Presented) The network apparatus according to claim 1, wherein the spoofing module is configured to allocate a connection control block among a plurality of connection control blocks corresponding to a spoofed connection, each of the plurality of connection control blocks storing information related to the plurality of connections, wherein the quantity of connection control blocks is configurable.

5. (Previously Presented) The network apparatus according to claim 1, wherein the backbone connection is a satellite link, the apparatus further comprising:

an encryption module configured to encrypt the satellite link.

6. (Original) The network apparatus according to claim 1, wherein the plurality of connections are established according to the Transmission Control Protocol (TCP).

7. (Previously Presented) The network apparatus according to claim 1, wherein the spoofing criteria includes at least one of Destination IP (Internet Protocol) address; Source IP address; TCP port numbers; TCP options; or IP differentiated services (DS) field.

8. (Previously Presented) The network apparatus according to claim 1, wherein the prioritization criteria includes at least one of Destination IP (Internet Protocol) address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

9. (Previously Presented) The network apparatus according to claim 1, wherein the prioritization module sets priority of one of the received messages, the one message being an IP (Internet Protocol) packet, wherein the path selection criteria includes at least one of the priority of the IP packet, Destination

IP address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

10. (Currently Amended) A method for performing functions to enhance performance of a communication network, the method comprising:

selectively spoofing a plurality of connections associated with a plurality of hosts based upon corresponding spoofing criteria;

providing local acknowledgement of received messages over the connections;

multiplexing the plurality of connections over a common backbone connection;

prioritizing access to the backbone connection based upon prioritization criteria;

determining a path among a plurality of paths to transmit the received messages based upon path selection criteria ; and

applying data compression on individual ones of the connections or the backbone connection using, concurrently, different types of compression on the individual connections.

11. (Previously Presented) The method according to claim 13, further comprising:

storing connection control block allocation information in a mapping table.

12. (Previously Presented) The method according to claim 13, further comprising:

outputting pointers corresponding to the plurality of connection control blocks.

13. (Previously Presented) The method according to claim 10, further comprising:

allocating a connection control block among a plurality of connection control blocks corresponding to a spoofed connection, each of the plurality of connection control blocks storing information

related to the plurality of connections, wherein the quantity of connection control blocks is configurable.

14. (Previously Presented) The method according to claim 10, wherein the backbone connection in the multiplexing step is a satellite link, the method further comprising:

encrypting the satellite link.

15. (Original) The method according to claim 10, wherein the plurality of connections in the step of selectively spoofing are established according to the Transmission Control Protocol (TCP).

16. (Previously Presented) The method according to claim 10, wherein the spoofing criteria in the step of selectively spoofing includes at least one of Destination IP (Internet Protocol) address; Source IP address; TCP port numbers; TCP options; or IP differentiated services (DS) field.

17. (Previously Presented) The method according to claim 10, wherein the prioritization criteria in the prioritizing step includes at least one of Destination IP address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

18. (Previously Presented) The method according to claim 10, further comprising:

setting priority of one of the received messages, the one message being an IP (Internet Protocol) packet, wherein the path selection criteria in the includes at least one of the priority of the IP packet, Destination IP address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

19. (Currently Amended) A network apparatus for performing functions to enhance performance of a communication network, the network apparatus comprising:

means for selectively spoofing a plurality of connections associated with a plurality of hosts based upon corresponding spoofing criteria;

means for providing local acknowledgement of received messages over the connections;

means for multiplexing the plurality of connections over a common backbone connection;

means for prioritizing access to the backbone connection based upon prioritization criteria;

means for determining a path among a plurality of paths to transmit the received messages based upon path selection criteria ; and

means for applying data compression on individual ones of the connections or the backbone connection using, concurrently, different types of compression on the individual connections.

20. (Previously Presented) The network apparatus according to claim 22, further comprising:

means for storing connection control block allocation information in a mapping table.

21. (Previously Presented) The network apparatus according to claim 22, further comprising:

means for outputting pointers corresponding to the plurality of connection control blocks.

22. (Previously Presented) The network apparatus according to claim 19, further comprising:

means for allocating a connection control block among a plurality of connection control blocks corresponding to a spoofed connection, each of the plurality of connection control blocks storing information related to the plurality of connections, wherein the quantity of connection control blocks is configurable.

23. (Previously Presented) The network apparatus according to claim 19, wherein the backbone connection is a satellite link, the apparatus further comprising:

means for encrypting the satellite link.

24. (Original) The network apparatus according to claim 19, wherein the plurality of connections are established according to the Transmission Control Protocol (TCP).

25. (Previously Presented) The network apparatus according to claim 19, wherein the spoofing criteria includes at least one of Destination IP (Internet Protocol) address; Source IP address; TCP port numbers; TCP options; or IP differentiated services (DS) field.

26. (Previously Presented) The network apparatus according to claim 19, wherein the prioritization criteria includes at least one of Destination IP address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

27. (Previously Presented) The network apparatus according to claim 19, wherein the prioritization module sets priority of one of the received messages, the one message being an IP (Internet Protocol) packet, wherein the path selection criteria includes at least one of the priority of the IP packet, Destination IP address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

28. (Currently Amended) A computer-readable medium carrying one or more sequences of one or more instructions for performing functions to enhance performance of a communication network, the

one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

selectively spoofing a plurality of connections associated with a plurality of hosts based upon corresponding spoofing criteria;

providing local acknowledgement of received messages over the connections;

multiplexing the plurality of connections over a common backbone connection;

prioritizing access to the backbone connection based upon prioritization criteria;

determining a path among a plurality of paths to transmit the received messages based upon path selection criteria ; and

applying data compression on individual ones of the connections or the backbone connection using, concurrently, different types of compression on the individual connections.

29. (Previously Presented) The computer-readable medium according to claim 31, wherein the one or more processors further perform the step of:

storing connection control block allocation information in a mapping table.

30. (Previously Presented) The computer-readable medium according to claim 31, wherein the one or more processors further perform the step of:

outputting pointers corresponding to the plurality of connection control blocks.

31. (Previously Presented) The computer-readable medium according to claim 28, wherein the one or more processors further perform the step of:

allocating a connection control block among a plurality of connection control blocks corresponding to a spoofed connection, each of the plurality of connection control blocks storing information

related to the plurality of connections, wherein the quantity of connection control blocks is configurable.

32. (Original) The computer-readable medium according to claim 28, wherein the backbone connection in the multiplexing step is a satellite link, and the one or more processors further perform the step of:

encrypting the satellite link.

33. (Original) The computer-readable medium according to claim 28, wherein the plurality of connections in the step of selectively spoofing are established according to the Transmission Control Protocol (TCP).

34. (Previously Presented) The computer-readable medium according to claim 28, wherein the spoofing criteria in the step of selectively spoofing includes at least one of Destination IP (Internet Protocol) address; Source IP address; TCP port numbers; TCP options; or IP differentiated services (DS) field.

35. (Previously Presented) The computer-readable medium according to claim 28, wherein the prioritization criteria in the prioritizing step includes at least one of Destination IP (Internet Protocol) address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP (User Datagram Protocol) port numbers, or IP differentiated services (DS) field.

36. (Previously Presented) The computer-readable medium according to claim 28, wherein the one or more processors further perform the step of:

setting priority of one of the received messages, the one message being an IP (Internet Protocol) packet, wherein the path selection criteria in the includes at least one of the priority of the IP packet,

Destination IP address, Source IP address, IP next protocol, TCP (Transmission Control Protocol) port numbers, UDP port numbers, or IP differentiated services (DS) field.